e. On or about April 13, 2017, Correia (using the Correia Yahoo Account) emailed Parnas (at the Parnas Yahoo Account) regarding certain communications with Victim-2.

f. In or about January and February 2018, Correia (using the Correia Yahoo Account), often copying Parnas (at the Parnas Yahoo Account), exchanged various emails with Victim-1, apparently concerning a potential different investment or transaction.

g. In or about March 2018, an investor in Fraud Guarantee ("Victim-5") exchanged emails with, among others, Correia (at the Correia Yahoo Account), concerning a $200,000 "loss" on his investment in Fraud Guarantee.

h. In or about July 2018, Parnas (at the Parnas Yahoo Account), along with Correia and others, received an invitation to participate in a phone call with a representative of [redacted] regarding Fraud Guarantee.

i. On or about September 18, 2018, Correia, blind copying Parnas (at the Parnas Yahoo Account), sent various Fraud Guarantee transactional documents to an investor in Fraud Guarantee ("Victim-4"). Several months later, on or about June 11, 2019, Correia forwarded this email to himself (at the Correia Yahoo Account).

j. On or about October 31, 2018, Correia emailed Parnas (at the Parnas Yahoo Account) concerning the negotiation of a Fraud Guarantee contract with [redacted]

k. In or about November 2018, Correia (using the Correia Yahoo Account) exchanged emails with Victim-1 regarding Victim-1's ownership stake in Fraud Guarantee.

l. In or about June 2019, Correia (using the Correia Yahoo Account), copying Parnas (at the Parnas Yahoo Account), exchanged emails with a third-party regarding certain unpaid expenses owed by Fraud Guarantee.

14. Therefore, there is probable cause to believe that the Parnas Yahoo Account and Correia Yahoo Account contain evidence of Correia's and Parnas's communications with each other regarding Fraud Guarantee, and with actual and potential victims of their fraudulent scheme.

15. Furthermore, based on my training and experience, email accounts like the Parnas Yahoo Account and Correia Yahoo Account, which have been used to communicate with others in furtherance of an unlawful fraudulent scheme, often contain records of that activity, including emails, chats, documents and multimedia (such as videos and photographs of documents or other evidence of criminality), payment records, contact information of co-conspirators and/or witnesses, notes about calls and meetings, calendar entries relating to calls and meetings, and internet search history relating to unlawful conduct. Additionally, email accounts like the Parnas Yahoo Account and Correia Yahoo Account often contain IP and location information, which can result in the creation of records of physical locations of meetings and calls. Individuals engaged in criminal activity often store such records in order to, among other things, keep track of co-conspirators' contact information, keep a record of requests for payments or of payments made, and follow-up on requests for payments, contributions, or other aspects of the schemes.

16. Accordingly, there is probable cause to believe that Subject Device-1, which contains content and information from the Parnas Yahoo Account and Correia Yahoo Account, will contain evidence of Parnas's and Correia's involvement in a fraudulent scheme involving Fraud Guarantee.

Subject Device-2
(Containing the Parnas iCloud Accounts)

17. Based on my review of electronic communications stored on the Parnas iCloud Accounts (obtained pursuant to the search warrants identified above), including text messages, iMessages, and WhatsApp messages, I have learned, in substance and in part, that Parnas engaged

in electronic communications with multiple individuals relevant to Fraud Guarantee. For example, the Parnas iCloud Accounts contain, among other things, evidence of communications between Parnas and (i) Correia, his principal co-conspirator in the Fraud Guarantee fraudulent scheme, (ii) Rudolph Giuliani, whom Parnas and Correia retained—through $500,000 paid by Victim-4—ostensibly to provide consulting services as to Fraud Guarantee, and (iii) various actual and potential investors in Fraud Guarantee, including Victim-1, Victim-2, Victim-3, Victim-4, Victim-5, and Intended Victim-1. These communications span from at least in or about early 2013 to in or about early 2019. Accordingly, there is probable cause to believe that these communications contain evidence and instrumentalities of the Subject Offenses, including discussions between Parnas and Correia concerning Fraud Guarantee and its business and operations (or lack thereof), discussions with Giuliani concerning his and his firm's work for Fraud Guarantee or other action taken in exchange for the $500,000 payment, and statements including representations or promises made to actual or potential victims of the fraudulent scheme.

18. Furthermore, based on my training and experience, iPhones like those linked to the Parnas iCloud Accounts, which have been used to communicate with others in furtherance of the Subject Offenses, often contain records of that activity, including call logs, voicemail messages, text messages, email correspondence, payment records, documents and multimedia (such as videos and photographs of documents or other evidence of criminality), contact information of co-conspirators and/or witnesses, notes about calls and meetings, internet search history relating to unlawful conduct, and logs of communication with co-conspirators and/or witnesses over messaging applications. Individuals engaged in criminal activity often store such records in order to, among other things, keep track of co-conspirator's contact information, keep a record of requests for payments or of payments made, and follow-up on requests for payments,

contributions, or other aspects of the schemes. Based on my training and experience, I also know that once records are backed up to an iCloud, they can exist there for months or even years after they were created, even if a user replaces an iPhone or removes files from an iPhone device. Indeed, I have learned from publicly-available information from Apple that, depending on a user's settings, even if a user removes files from an iPhone, that user would need to log into their iCloud account and manually delete those same files in order for them to be removed from the iCloud account. Accordingly, there is reason to believe that records will be found in the Parnas iCloud Accounts that date back years.

19. Accordingly, there is probable cause to believe that Subject Device-2, which contains content and information from the Parnas iCloud Accounts, will contain evidence of Parnas's and Correia's involvement in a fraudulent scheme involving Fraud Guarantee.

Subject Device-3 and Subject-Device-4
(Containing the Parnas iPhone 11 and Correia iPhone, Respectively)

20. Based on my review of electronic communications stored on the Parnas iCloud Accounts (obtained pursuant to the search warrants identified above), including text messages, iMessages, and WhatsApp messages, I have learned, in substance and in part, that Parnas used the Parnas Numbers associated with the Parnas iPhone 11 and Correia used the Correia Number associated with the Correia iPhone to engage in electronic communications with multiple individuals relevant to Fraud Guarantee. For example, the Parnas iCloud Accounts contain, among other things, evidence of communications between Parnas (using the Parnas Numbers) and Correia (using the Correia Number). The Parnas iCloud Accounts also contain evidence that the Parnas Numbers were used to send and receive group text messages amongst Parnas, Correia (using the Correia Number), and various actual and potential investors in Fraud Guarantee, including Victim-1, Victim-2, Victim-3, Victim-4, Victim-5, and Intended Victim-1. Accordingly, it appears that

much of the material stored on the Parnas iCloud Accounts was sent or received using the Parnas Numbers and therefore likely came from the Parnas iPhone 11. Thus, because (as set forth above) there is probable cause to believe that the Parnas iCloud Accounts contain evidence of Parnas's electronic communications with various individuals relevant to the Fraud Guarantee scheme, there is likewise probable cause to believe that evidence of such communications exists on Subject Device-3, which contains content and information from the Parnas iPhone 11.

21. Based on my review of documents produced by Victim-3, I have learned, in substance and in part, that Victim-3 engaged in extensive text message communications with Correia (who was using the Correia Number, which is associated with the Correia iPhone) concerning Fraud Guarantee, among other subjects, between at least in or about October 2016 and in or about October 2019. I have also learned from the CEO—including through my review of materials produced by him—that he was likewise in communication with Correia regarding Fraud Guarantee via text message between at least in or about early 2016 and late 2018. In addition, based on my review of documents produced by Victim-4, I have learned, in substance and in part, that Victim-4 exchanged text messages with Correia, concerning Victim-4's then-impending investment in Fraud Guarantee, between in or about September 16 and September 19, 2018.

22. Based on my review of technical information provided by Apple, I know that when an individual acquires a new iPhone, it is possible to transfer data from an old device to the new iPhone. Further, based on my training and experience, individuals regularly transfer such data so that they can have access to their contacts, messages, notes, calendar entries, and pictures, among other data. Accordingly, there is probable cause to believe that the Parnas iPhone 11 and Correia iPhone were used to send and receive the messages described above, or contain the backup or

transferred content from iPhones, and therefore are likely to contain evidence of Parnas's and Correia's electronic communications with these individuals.

23. In addition, based on my training and experience, individuals who engage in offenses such as the Subject Offenses often store records relating to their illegal activity and to persons involved with them in that activity on electronic devices such as the Parnas iPhone 11 and Correia iPhone. Such records can include, for example, logs of online chats or text messages or phone calls with co-conspirators; photographs, email correspondence and other communications (including via third-party messaging applications) with co-conspirators; contact information of co-conspirators, including telephone numbers, email addresses, and/or identifiers for instant messaging and social media accounts; financial data, including bank account numbers; and/or documents and drafts of documents used or contemplated for use in furtherance of the scheme.

24. Accordingly, there is probable cause to believe that Subject Device-3 and Subject Device-4, which contain content and information from the Parnas iPhone 11 and Correia iPhone, respectively, will contain evidence of Parnas's and Correia's involvement in a fraudulent scheme involving Fraud Guarantee.

* * *

25. Time limitation: To the extent materials are dated, this search warrant application is limited to all content created, sent, or received on or after September 1, 2013, which is shortly before Correia registered Fraud Guarantee in Delaware, to the present.

A. Evidence, Fruits and Instrumentalities

26. Based upon the foregoing, I respectfully submit there is probable cause to believe that the Subject Devices will contain evidence, fruits, and instrumentalities of the Subject Offenses, as more fully described in Section II of Attachment A to the proposed warrant.

27. In particular, I believe the Subject Devices are likely to contain the following information:

a. Evidence relating to, including communications with, Rudolph Giuliani, [redacted] and any actual or potential investors, members, or partners of Fraud Guarantee;

b. Evidence relating to Fraud Guarantee's plans, finances, assets, and operations, or lack thereof, including any corporate books and records;

c. Evidence relating to Fraud Guarantee's actual or prospective business relationships, including but not limited to business relationships with any insurance carriers;

d. Evidence relating to Fraud Guarantee's members, officers, directors, investors, partners, employees, agents, consultants, affiliates, subsidiaries, and associates.

e. Evidence relating to the nature and extent of Rudolph Giuliani's and [redacted] work on behalf of Parnas, Correia, and/or Fraud Guarantee, or lack thereof, including any evidence of Giuliani's efforts to assist in the removal of Ambassador [redacted] and whether or not such efforts benefited Fraud Guarantee;

f. Evidence relating to any efforts by Parnas, Correia, their family members, or others associated with Fraud Guarantee in receiving, transferring, withdrawing, or otherwise using any monetary funds or instruments;

g. Evidence relating to the use of monetary funds or instruments paid to Fraud Guarantee, Parnas, or Correia to make political contributions;

h. Evidence of meetings between Parnas, Correia, Giuliani, and any actual or potential investors in Fraud Guarantee, including but not limited to travel records, and location and IP records;

i. Evidence of the existence of email accounts, iCloud accounts, or electronic devices used by Parnas, Correia or others associated with Fraud Guarantee to communicate with actual or potential investors, or co-conspirators;

j. Passwords or other information needed to access user's online accounts.

IV. Procedures for Searching ESI

A. Review of ESI

28. Law enforcement personnel (including, in addition to law enforcement officers and agents, and depending on the nature of the ESI and the status of the investigation and related proceedings, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, interpreters, and outside vendors or technical experts under government control) will review the ESI contained on the Subject Devices for information responsive to the warrant.

29. In conducting this review, law enforcement personnel may use various techniques to determine which files or other ESI contain evidence or fruits of the Subject Offenses. Such techniques may include, for example:

- surveying directories or folders and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);
- conducting a file-by-file review by "opening" or reading the first few "pages" of such files in order to determine their precise contents (analogous to performing a cursory examination of each document in a file cabinet to determine its relevance);
- "scanning" storage areas to discover and possibly recover recently deleted data or deliberately hidden files; and

- performing electronic keyword searches through all electronic storage areas to determine the existence and location of data potentially related to the subject matter of the investigation[1]; and

- reviewing metadata, system information, configuration files, registry data, and any other information reflecting how, when, and by whom the computer was used.

30. Law enforcement personnel will make reasonable efforts to restrict their search to data falling within the categories of evidence specified in the warrant. Depending on the circumstances, however, law enforcement personnel may need to conduct a complete review of all the ESI from seized devices or storage media to evaluate its contents and to locate all data responsive to the warrant.

[1] Keyword searches alone are typically inadequate to detect all relevant data. For one thing, keyword searches work only for text data, yet many types of files, such as images and videos, do not store data as searchable text. Moreover, even as to text data, there may be information properly subject to seizure but that is not captured by a keyword search because the information does not contain the keywords being searched.

V. Conclusion and Ancillary Provisions

31. Based on the foregoing, I respectfully request the court to issue a warrant to seize the items and information specified in Attachment A to this affidavit and to the Search and Seizure Warrant.

32. In light of the confidential nature of the continuing investigation, I respectfully request that this affidavit and all papers submitted herewith be maintained under seal until the Court orders otherwise.

[redacted]

Sworn to before me on
21st day of January, 2020

HON. J. PAUL OETKEN
UNITED STATES DISTRICT JUDGE

Attachment A

I. Devices to be Searched

The devices to be searched ("Subject Device-1," "Subject Device-2," "Subject Device-3," and "Subject Device-4," and collectively, the "Subject Devices") are described as four hard drive partitions containing the following content and information obtained pursuant to the following prior search warrants:

Account/Device	Previously searched pursuant to search warrant(s)	Referred to as
SUBJECT DEVICE-1		
[redacted]	19 Mag. 729 (Jan. 18, 2019) 19 Mag. 7593 (Aug. 14, 2019)	Parnas Yahoo Account
	19 Mag. 7595 (Oct. 17, 2019)	Correia Yahoo Account
SUBJECT DEVICE-2		
Parnas iCloud account number [redacted]	19 Mag. 4784 (May 16, 2019) 19 Mag. 9829 (Oct. 21, 2019)	Parnas iCloud Accounts
iCloud account number [redacted]	19 Mag. 9832 (Oct. 21, 2019)	
SUBJECT DEVICE-3		
Black iPhone 11 with the serial number [redacted] seized from Lev Parnas incident to his arrest at Dulles International Airport on Oct. 9, 2019	19 Mag. 9832 (Oct. 21, 2019)	Parnas iPhone 11
SUBJECT DEVICE-4		
iPhone with the serial number [redacted] seized from a package sent by David Correia via DHL	19 Mag. 9830 (Oct. 21, 2019)	Correia iPhone

II. Review of ESI on the Subject Devices

Law enforcement personnel (including, in addition to law enforcement officers and agents, and depending on the nature of the ESI and the status of the investigation and related proceedings, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, interpreters, and outside vendors or technical experts under government control) are authorized to review the ESI contained on the Subject Devices for evidence, fruits, and instrumentalities of one or more violations of 18 U.S.C. § 1343 (wire fraud) and § 1349 (attempting and/or conspiring to commit wire fraud) (together, the "Subject Offenses"), limited to content created, sent, or received between September 1, 2013 and the date of this warrant, as listed below:

a. Evidence relating to, including communications with, Rudolph Giuliani [redacted]s, and any actual or potential investors, members, or partners of Fraud Guarantee;

b. Evidence relating to Fraud Guarantee's plans, finances, assets, and operations, or lack thereof, including any corporate books and records;

c. Evidence relating to Fraud Guarantee's actual or prospective business relationships, including but not limited to business relationships with any insurance carriers;

d. Evidence relating to Fraud Guarantee's members, officers, directors, investors, partners, employees, agents, consultants, affiliates, subsidiaries, and associates.

e. Evidence relating to the nature and extent of Rudolph Giuliani's and [redacted] work on behalf of Parnas, Correia, and/or Fraud Guarantee, or lack thereof, including any evidence of Giuliani's efforts to assist in the removal of Ambassador [redacted] and whether or not such efforts benefited Fraud Guarantee;

f. Evidence relating to any efforts by Parnas, Correia, their family members, or others associated with Fraud Guarantee in receiving, transferring, withdrawing, or otherwise using any monetary funds or instruments;

g. Evidence relating to the use of monetary funds or instruments paid to Fraud Guarantee, Parnas, or Correia to make political contributions;

h. Evidence of meetings between Parnas, Correia, Giuliani, and any actual or potential investors in Fraud Guarantee, including but not limited to travel records, and location and IP records;

i. Evidence of the existence of email accounts, iCloud accounts, or electronic devices used by Parnas, Correia or others associated with Fraud Guarantee to communicate with actual or potential investors, or co-conspirators;

j. Passwords or other information needed to access user's online accounts.

EXHIBIT A

19 MAG 11651

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

In the Matter of a Warrant for All Content and Other Information Associated with the Email Accounts [redacted] and [redacted], Maintained at Premises Controlled by Google, LLC, USAO Reference No. [redacted]

TO BE FILED UNDER SEAL

AGENT AFFIDAVIT

Agent Affidavit in Support of Application for a Search Warrant for Stored Electronic Communications

STATE OF NEW YORK)
) ss.
COUNTY OF NEW YORK)

[redacted] being duly sworn, deposes and states:

I. Introduction

A. Affiant

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI"). In the course of my experience and training in this position, I have participated in criminal investigations into federal offenses involving public corruption, including wire fraud and violations of the federal campaign finance laws. I also have training and experience executing search warrants, including those involving electronic evidence.

B. The Provider, the Subject Accounts and the Subject Offenses

2. I make this affidavit in support of an application for a search warrant pursuant to 18 U.S.C. § 2703 for all content and other information associated with the email accounts [redacted] ("Subject Account-1") and [redacted] ("Subject Account-2") (together, the "Subject Accounts"), maintained and controlled by Google, LLC (the